LIVRE BLANC

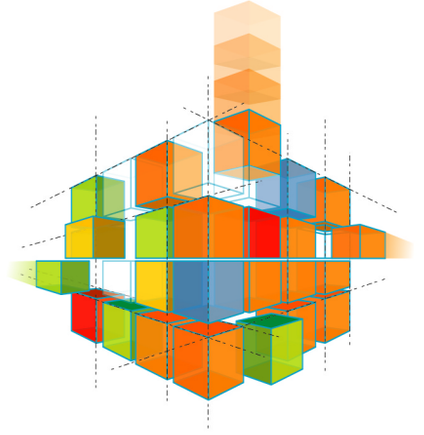
FÉVRIER 2006

TÉLÉPHONIE & IP

UNE CONVERGENCE À DISCIPLINER

ARKOON NETWORK SECURITY

En France, une entreprise sur trois a un projet de convergence voix-données. Cette évolution implique des changements au niveau de l'infrastructure, des serveurs et des terminaux. La sécurité et la qualité de service s'avèrent déterminantes pour la réussite du projet de téléphonie IP.



ADAPTIVE SECURITY

AMC SSL360 FAST360 Security BOX

MAÎTRISEZ LES VULNÉRABILITÉS DE LA TÉLÉPHONIE IP AVEC ARKOON

POUR BÉNÉFICIER DES GAINS DE LA ToIP, L'ENTREPRISE DOIT ANALYSER LES ÉVOLUTIONS DU MARCHÉ ET DES TECHNOLOGIES.

En Europe, moins de deux entreprises sur dix utilisent déjà la voix au dessus des protocoles Internet. On en prévoit deux fois plus d'ici à la fin 2008. Toutes les entreprises ne partent pas du même existant : à peine plus d'un autocommutateur installé sur deux supporte IP en plus des lignes traditionnelles.

Par conséquent, la cohabitation entre voix traditionnelle (dite « TDM ») et voix IP, bien amorcée, va se poursuivre durant plusieurs années encore. Elle peut s'effectuer au sein de l'entreprise, à l'extérieur, via une offre d'opérateur, ou même de façon mixte. C'est pourquoi on parle de convergence de téléphonie et d'applications IP, autour des PBX, des programmes de gestion d'appels (CTI, ACD, messagerie unifiée), des téléphones (fixes ou sans fil) et des softphones, ces logiciels clients de téléphonie pour PC.

Les prestataires du déploiement proviennent de deux cultures différentes : celle de la voix d'une part (aux nombreux protocoles propriétaires), et celle des données d'autre part, prônant l'interopérabilité des équipements et l'évolution des solutions par logiciels. On dénombre autour des produits de téléphonie IP plusieurs protocoles, dont certains demeurent propriétaires tel le SCCP de Cisco Systems. En outre, la voix peut être « cachée » dans des flux HTTP de données traditionnelles. Protéger la téléphonie IP implique donc une analyse des protocoles et un examen soigné des paquets, au delà du scan des ports et des adresses IP réalisé par le pare-feu.

Maîtriser les failles de sécurité de la ToIP signifie contrôler des vulnérabilités en interne comme en externe. Sans oublier les protections de base que sont l'onduleur, la ligne téléphonique de secours, la redondance des équipements critiques et celle des liens vers le réseau public.

PROTÉGER GLOBALEMENT

La protection de la convergence voix-données repose sur quatre piliers principaux. D'abord, l'aiguillage conforme des flux selon leur typologie permet de garder le contrôle de la VoIP. Il faut différencier les flux de la voix « officielle », c'est à dire supportée par le PABX de l'entreprise, de ceux de la voix générée par exemple par le logiciel P2P Skype. Pour cela, on doit pouvoir analyser finement le contenu des paquets IP. En second, la coupure d'appel téléphonique peut s'effectuer dès l'initialisation de l'appel ou en cours de communication. Une absence d'authentification ou un changement de Codec en cours de conversation pourront déclencher cette protection. Troisièmement, la sécurité devient collaborative : des échanges d'informations en temps réel sont nécessaires entre les équipements purement réseau et ceux au plus près du PBX, pour couper un appel illicite par exemple. Arkoon prend en compte cette dualité TDM & IP avec son partenaire CheckPhone. Un cloisonnement s'effectue, d'une part, entre les flux de données et les flux de la voix et, d'autre part, entre la voix officielle et la voix spontanée, bloquée le cas échéant.

Quatrième pillier, la mise en œuvre de la gestion de la qualité de service garantit que les flux VoIP font l'objet d'une priorité adéquate. Cette mise en œuvre intervient seulement après la phase d'analyse pour ne gérer que les flux répondant aux critères pré-établis par l'entreprise.

CONTRÔLE DES FLUX

Les appliances Arkoon détectent et contrôle les flux des réseaux convergents. Performantes, elles permettent l'aiguillage des flux, la coupure d'appels illicites en relation avec le PBX, la mise en œuvre de la qualité de service et de règles de sécurité. Le tunneling des flux VoIP (via les tunnels VPN des liens intersites de l'entreprise) aide à gérer un PBX distant du centre de traitements.

VOIX ET DONNÉES INFORMATIQUES, SEPT MENACES À SURVEILLER

UNE FOIS LES VULNÉRABILITÉS DE LA ToIP IDENTIFIÉES, L'ENTREPRISE DOIT PLANIFIER PUIS SUPERVISER LES FLUX VOIX-DONNÉES TRANSMIS SUR SON INFRASTRUCTURE.

UN FRANÇAIS AU SECOURS DE LA ToIP

Arkoon offre une gamme complète d'équipements de sécurité.

En combinant les avantages de la téléphonie traditionnelle aux infrastructures et services Internet, la téléphonie sur IP fournit de nombreuses opportunités à l'entreprise. Elle réduit ses coûts de communications, améliore la productivité des équipes et leur disponibilité, par exemple en consolidant le centre de contacts. La ToIP (Telephony over IP) prolonge le lien des collaborateurs du siège avec les employés sur le terrain, en déplacement ou en télétravail. Grâce à sa gestion de présence, on peut joindre ses interlocuteurs où qu'ils soient, sur leur combiné fixe ou mobile ou sur le logiciel softphone de leur ordinateur. Du coup, la gestion du temps et les projets professionnels gagnent en efficacité.

A la faveur d'un déménagement ou lorsqu'elle renouvelle son autocommutateur, l'entreprise examine les solutions ToIP. Mais faire converger la voix et les données sur une même infrastructure pose une nouvelle question : comment écarter les risques introduits par la téléphonie IP ?

Les vulnérabilités (voir ci-contre) imposent à l'entreprise de nouvelles précautions. Une analyse des risques et de leur impact sur les métiers aide à retenir les parades adéquates. On distingue trois zones de menaces principales, liées à la convergence des applications informatiques et de téléphonie : l'infrastructure peut d'abord devenir la cible d'un contournement de ressources – elle servira des appels incontrôlés par exemple. Les services de téléphonie sur IP peuvent être paralysés ou bloqués en partie par une intrusion. Enfin, les contenus numériques de l'entreprise, comme son annuaire ou ses conversations confidentielles, peuvent faire l'objet de vol d'informations. Arkoon est un spécialiste de la sécurité des réseaux IP. L'entreprise française offre une voie de migration sûre vers la Téléphonie IP, sans remise en cause des investissements préalablement consentis – pour le pare-feu réseau en particulier. L'approche multicouche d'Arkoon aide l'entreprise à faire converger les services voix et données en toute sécurité, sans risque de subir intrusions, dénis de service ou fuites d'informations.

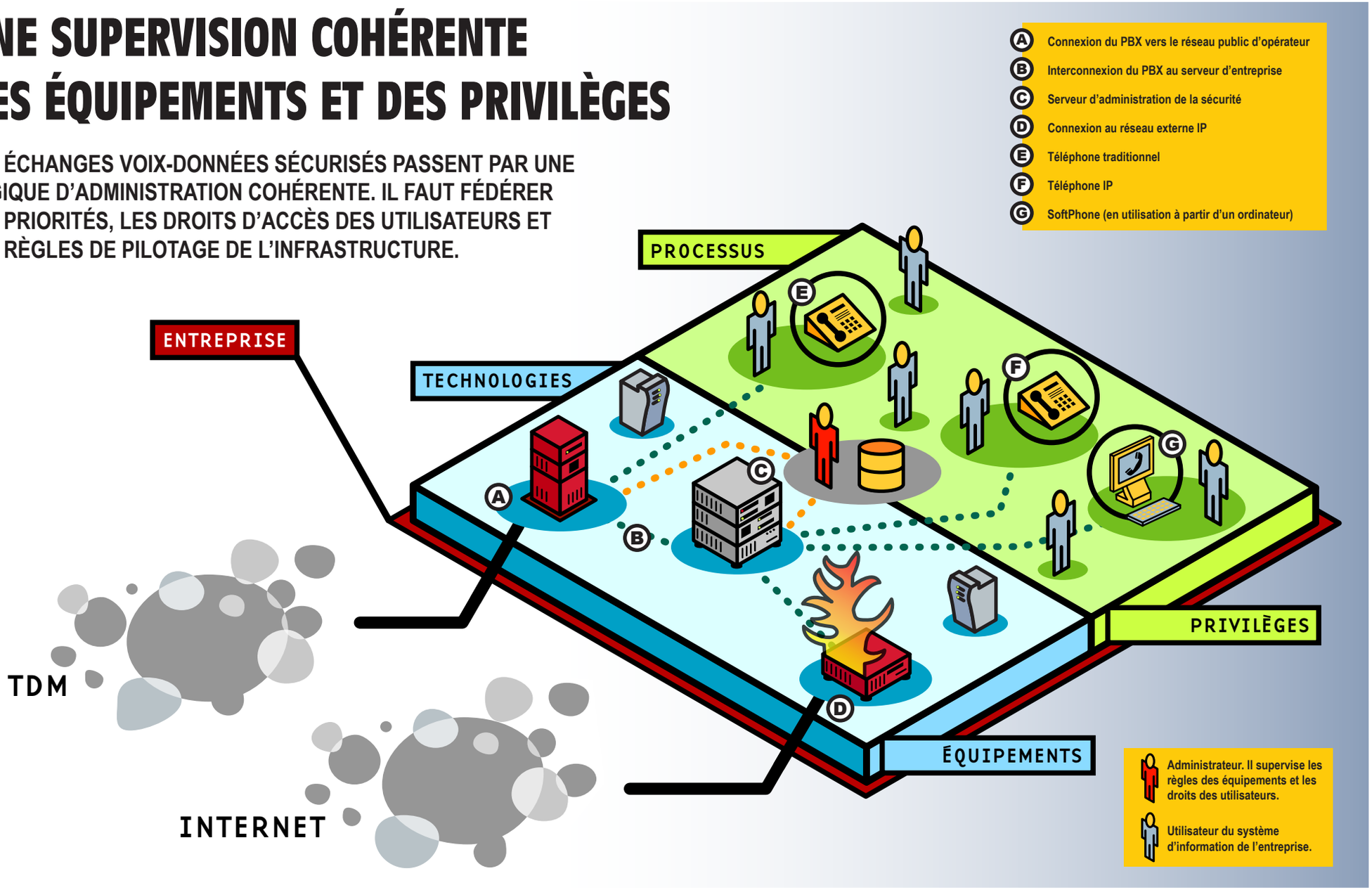
L'entreprise doit traiter la voix comme une application critique et assurer sa sécurisation comme elle le fait pour ses programmes existants. Pour héberger des échanges incorruptibles, l'infrastructure doit évoluer en fiablilité et en factulté d'administration. Il faut améliorer la qualité des services et la sécurité des échanges simultanément.

MENACES	CIBLES*	VISIBLES	IMPACTS	PRÉREQUIS	PARADES TECHNIQUES
Déni de service ToIP	I, S	Oui	Service téléphonique	Echanges avec le PBX (administration)	Pare-feu Prévention d'intrusions
Usurpation d'identité	I, S	Non	Intégrité des échanges	Annuaire	Authentification
Détournement de messages vocaux	S,C	Non	Intégrité des échanges Confidentialité	Règles de filtrage	Authentification Pare-feu applicatif
Vol d'annuaire	I, S, C	Non	Confidentialité	Règles de filtrage	Authentification Pare-feu applicatif
SPIT (messages non sollicités)	I, S, C	Oui	Service téléphonique Baisse de productivité	Echanges avec le PBX (administration)	Authentification, Pare-feu applicatif Prévention d'intrusions
Détournement de service applicatif	S, C	Non	Perte de contrôle Consommation de ressources	Politique de sécurité Configuration	Pare-feu applicatif
Détournement d'infrastructure	I	Non	Perte de contrôle Confidentialité	Définitions de rôles administrateurs et utilisateurs	Facultés d'audit Pare-feu applicatif

* I = Infrastructures, S = Services, C = Contenus

UNE SUPERVISION COHÉRENTE DES ÉQUIPEMENTS ET DES PRIVILÈGES

LES ÉCHANGES VOIX-DONNÉES SÉCURISÉS PASSENT PAR UNE LOGIQUE D'ADMINISTRATION COHÉRENTE. IL FAUT FÉDÉRER LES PRIORITÉS, LES DROITS D'ACCÈS DES UTILISATEURS ET LES RÈGLES DE PILOTAGE DE L'INFRASTRUCTURE.



TROIS POLITIQUES À SUIVRE POUR PROTÉGER TOUTES LES COMMUNICATIONS DE L'ENTREPRISE

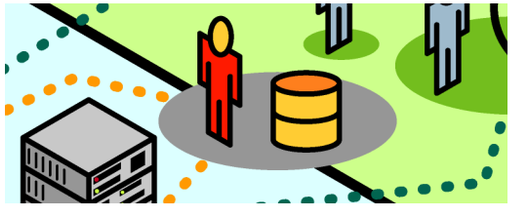
DES PROCESSUS BIEN DÉFINIS, DES ÉQUIPEMENTS SUPERVISÉS ET UNE STRATÉGIE DE SEGMENTATION DURCISSENT L'INFRASTRUCTURE ET LES COMMUNICATIONS SUPPORTANT LES ÉCHANGES VOIX-DONNÉES.

1 POLITIQUE HUMAINE

La sécurité est un processus qui consiste à définir puis propager des règles d'entreprise. On peut le faire en trois étapes. Tout d'abord, on définit une politique propre à chaque fonction dans l'entreprise. Les salariés, les consultants et les stagiaires ont chacun des tâches distinctes. Certains peuvent accéder aux ressources partagées, appeler les téléphones fixes ou mobiles à toute heure de la journée, mais pas tous. Une fois ces règles de collaboration établies, la politique humaine aide à dicter qui peut appeler qui, où, quand et comment ? Cette étape organisationnelle s'avère fondamentale pour sécuriser la téléphonie d'entreprise.

2 POLITIQUE D'ADMINISTRATION

Le décideur informatique choisit ses collaborateurs, ses serveurs et ses équipements de réseaux soigneusement. Les uns comme les autres vont l'aider à organiser et à optimiser le système d'informations de l'entreprise. Charge à lui de déterminer qui peut administrer quoi, quand, comment et depuis où ? Cette politique d'administration forme une étape indispensable. Elle impose des astreintes aux techniciens et aussi quelques limitations aux équipements. Elle n'en demeure pas moins essentielle pour que chaque collaborateur puisse placer toute sa confiance dans l'infrastructure et dans ses services. Et pour que chacun respecte les politiques locales et globales précisées dans la charte de sécurité.



3 POLITIQUE DE SEGMENTATION

Les réseaux d'entreprise évoluent avec la convergence de la voix et des données mais aussi et surtout avec la convergence des services informatiques, Internet et de téléphonie. Une politique de segmentation en sous-réseaux (ou VLAN) permet d'isoler les échanges de données par groupes de travail. Une approche semblable va isoler la voix officielle des échanges vocaux non supportés par l'entreprise. Une fois ce tri effectué, on peut garantir la sécurité et la confidentialité des échanges. Il faut s'assurer que les règles propres aux trois politiques (humaines, d'administration et de segmentation) soient distribuées à tous les équipements de l'infrastructure.

CLOISONNER AVANT D'OPTIMISER

NICOLAS BÉLAN,
Responsable du programme convergence chez Arkoon

Lorsque l'entreprise veut migrer vers la téléphonie IP, c'est souvent pour des raisons économiques. La sécurité passe après. Or, c'est exactement l'inverse qu'il faut faire : soigner la sécurité avant de gérer la qualité de services du réseau. Cloisonner d'abord et optimiser ensuite les flux. Sinon, la QoS va optimiser des trafics éventuellement malicieux. Il faut conserver une séparation entre le réseau IP de données et la VoIP, car les deux flux n'ont pas les mêmes besoins. La voix exige un très faible temps de latence de bout en bout, pas l'e-mail. En faisant converger deux réseaux séparés, l'entreprise doit éviter de combiner leurs problèmes de sécurité. Arkoon propose une appliance capable d'identifier la voix sur IP. C'est un équipement utile au cloisonnement et au contrôle des flux de l'infrastructure d'entreprise. Il faut néanmoins l'accompagner d'une politique de sécurité et s'assurer que les règles d'accès et de confidentialité soient bien respectées.

TÉLÉTRAVAILLEURS ET COLLABORATEURS DISTANTS RÉPONDENT À L'APPEL

COMMENT RESTER JOIGNABLE POUR SES CLIENTS ET SES COLLÈGUES LORSQU'ON EST EN DÉPLACEMENT OU EN TÉLÉTRAVAIL ? ARKOON ET PANASONIC CONCRÉTISENT CE DOUBLE OBJECTIF.

L'entreprise veut préserver l'intégrité de ses échanges et améliorer sa disponibilité et sa qualité de services. Pour concilier ces objectifs, avec des collaborateurs de plus en plus mobiles, la téléphonie IP s'avère précieuse. Les collaborateurs en déplacement ou en télétravail peuvent être joints comme s'ils étaient présents au siège de l'entreprise. En outre, la ToIP apporte une économie d'échelle en centralisant l'exploitation des ressources informatiques et de téléphonie. Sécurisée, elle procure aux clients et aux collaborateurs de meilleures réponses, plus rapides et plus précises.

L'équipementier Panasonic propose une gamme d'autocommutateurs IP (IPBX) ainsi qu'une connexion des travailleurs distants au système d'informations, deux briques essentielles de la téléphonie IP. « *Conscients que la ToIP est avant tout le marché des opérateurs, nous ciblons les entreprises de 10 à 200 postes en leur permettant d'investir graduellement* », explique Laurent Poirot, le responsable du département PBX de Panasonic France. Selon lui, la sécurité des échanges reste un paramètre indispensable. Il faut assurer, en particulier, l'authentification des utilisateurs. En effet, suite à l'identification d'un appel, une remontée de fiche automatique délivre l'historique commercial ou technique d'un client. On doit donc s'assurer d'aiguiller ces informations vers les seuls collaborateurs, locaux ou distants, de confiance. « *Souvent négligée, la sécurisation de la téléphonie IP s'avère cruciale* », confirme-t-il.

« TROP SOUVENT NÉGLIGÉE, LA SÉCURISATION DE LA ToIP S'AVÈRE CRUCIALE »

Pour faire converger les applications informatiques et la téléphonie, on peut brancher le combiné IP entre le réseau local et le PC, relié alors via une prise USB, en suivant l'approche first party de Panasonic. Autre possibilité, dite third party, utiliser un port Ethernet pour chaque terminal, ce qui oblige à redimensionner le réseau. Dans les deux cas, la sécurisation des équipements ne doit pas être négligée.

Partenaires des principaux éditeurs de logiciels de gestion de la relation client, Panasonic sait établir le dialogue entre le serveur applicatif et le central téléphonique, perçu comme un client du réseau informatique. Les protocoles TAPI 2 et CSTA sont disponibles en version de base, sur toute sa gamme de PBX, jusqu'au modèle KX-TDA 600 qui couvre les besoins de communication jusqu'à 1000 postes par site.

« *Ce qui intéresse surtout l'entreprise occidentale, à présent, c'est de gagner en réactivité, en compétitivité et en mobilité. La ToIP lui permet de s'affranchir de la distance des collaborateurs* ». Elle gomme également les décalages horaires, une entreprise internationale pouvant basculer ses appels vers une filiale étrangère pour rester toujours disponible pour ses clients, par-delà les continents et les heures ouvrées.

Dans les grandes chaînes d'hôtels, les outils de CRM (Customer Relationship Management) optimisent la qualité de l'accueil. Ailleurs, la ToIP s'étend aux collaborateurs distants et aux télétravailleurs, afin qu'ils puissent répondre aux attentes des clients. Parfois, un serveur vocal interactif s'immisce dans la chaîne de services IP, interrogeant le gestionnaire de données de l'entreprise, à distance. Avec le soutien des solutions Arkoon, l'autocommutateur IP et les serveurs d'applications deviennent des dispositifs du réseau comme les autres. Ils répondent enfin aux règles de sécurité fixées par l'entreprise.

Des processus critiques – les traitements de la logistique, le suivi des clients et des livraisons – s'appuient maintenant sur la téléphonie IP. Dans ce contexte, l'authentification des utilisateurs du système convergent devient indispensable. Pour apporter un retour rapide sur investissement, la ToIP doit supporter la voix et les échanges de données, savoir aiguiller les appels et les données clients et gérer un ensemble de services pertinents pour les collaborateurs distants. En intégrant le PBX-IP et les serveurs d'applications convergentes, les solutions d'Arkoon délivrent des échanges en temps réel, conformes aux priorités de l'entreprise.

GLOSSAIRE DE LA ToIP

ARCEP : Autorité de régulation des communications électroniques et des postes (ex-ART).

DoS : Denial of Service. Déni de service.

DMZ : Zone démilitarisée. Sous-réseau généralement entouré de pare-feux, dont les serveurs restent accessibles depuis l'extérieur de l'entreprise.

FIRECONVERGE : Cette interface intelligente permet l'inspection de la voix sur IP et celle de la voix traditionnelle. Elle est placée entre les équipements UTM d'Arkoon et la plate-forme ETSS de Checkphone.

GATEWAY : Passerelle de communication.

H.323 : Jeu de protocoles de l'UIT (Union Internationale des Télécommunications) permettant d'établir des échanges téléphoniques sur IP ainsi que les vidéoconférences.

IPBX : IP-based Private Branch eXchange. Autocommutateur gérant les appels au sein de l'entreprise. Utilisé sur un réseau IP, il autorise les appels et assure la commutation des paquets VoIP.

MGCP : Media Gateway Control Protocol. Egalement connu sous le nom Megaco (IETF) ou H.248 (ITU), ce protocole asymétrique gère la signalisation et la gestion des sessions lors d'une conférence IP multimédia.

PBX : Private Branch eXchange. Autocommutateur téléphonique ou équipement de commutation reliant les téléphones de l'entreprise au réseau TDM.

QoS : Quality of Service. Possibilité offerte par certains équipements du réseau (IP ou ATM) pour garantir par avance une transmission de données, son taux d'erreur et ses caractéristiques.

RTCP : Real-time Transfer Protocol. Protocole de contrôle des flux conçu pour assurer la qualité de service de sessions en temps réel.

SIP : Session Initiation Protocol. Ce protocole symétrique de l'IETF authentifie et localise les participants puis négocie les chemins de données utilisables.

SOFTPHONE : Logiciel, géré ou non par un IPBX, regroupant les fonctions d'un téléphone sur un micro-ordinateur relié au réseau Internet.

SPIT : Spam over Internet Telephony. Appels non sollicités polluant la boîte de messages vocaux.

TDM : désigne la technique de multiplexage Time Division Multiplexing et, plus généralement, les réseaux publics commutés d'opérateurs retenant cette technique.

ToIP : Telephony over IP. Téléphonie sur IP.

UTM : Unified Threat Management. Equipement de sécurité capable de gérer plusieurs types de menaces ou d'intrusions sur le réseau de l'entreprise. Il intègre des fonctions antivirus, pare-feu, pare-feu applicatif, une passerelle VPN, un logiciel IDS...

VLAN : Virtual LAN. Segment de réseau local virtuel.

VoIP : Voice over IP. Voix sur IP.

ARKOON MEMBRE DE VOIPSA

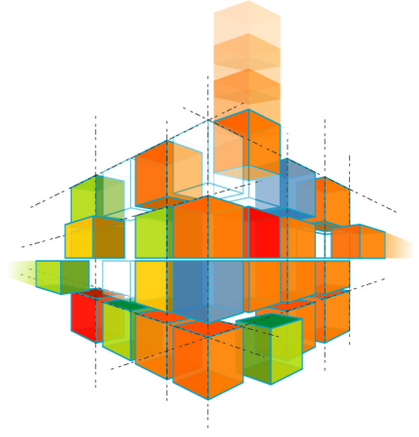
Créée en février 2005, l'alliance VOIPSA (Voice over IP Security Alliance) sensibilise le marché aux enjeux des réseaux convergents. En particulier, elle s'attache aux meilleures pratiques relatives à la sécurité et à la confidentialité. Les grands équipementiers, fournisseurs de services et chercheurs en sécurité informatique en sont membres. 3Com et sa filiale TippingPoint sont à l'origine de l'alliance. Ils ont été rapidement rejoints par Arkoon, Alcatel, SonicWall, Netcentex et Spirent, entre autres. L'objectif consiste à aider les entreprises à comprendre et à contrer les risques à travers des forums de discussion (tel le groupe de discussion VOIPSEC), mais aussi au travers de livres blancs sur la sécurité et sur la voix sur IP. En pratique, les groupes de travail VoIP Security Threat Taxonomy et Security Requirements proposent une liste complète des menaces liées aux applications de téléphonie sur IP, comme les attaques par saturation, l'exploitation de vulnérabilités des protocoles, l'usurpation d'identité, l'écoute ou la modification de flux audio. Une structure détaillée des failles techniques est ainsi décrite. L'alliance soutient aussi des projets d'études sur la sécurité, en développant des méthodologies, voire des outils gratuits. Elle propose enfin une liste de problèmes à prendre en compte par les services législatifs, en cas de besoin.

Pour en savoir plus : www.voipsa.org

POUR EN SAVOIR PLUS

ARKOON
NETWORK SECURITY

Sécuriser la convergence voix/données ne signifie pas protéger les données puis la voix. Il s'agit plutôt de distinguer la voix des données puis de filtrer la voix, conformément aux règles de l'entreprise.



ADAPTIVE SECURITY

SIÈGE SOCIAL
1 PLACE VERRAZZANO
CS 30603
69258 LYON CEDEX 09
TÉL : +33 (0)4 72 53 01 01
FAX : +33 (0)4 72 53 12 60

ILE DE FRANCE
IMMEUBLE LE PELISSIER
220 AV. PIERRE BROSSOLETTE
92240 MALAKOFF
TEL : +33 (0)1 57 63 67 00
FAX : +33 (0)1 57 63 67 37

www.arkoon.net / info@arkoon.net

AMC SSL360 FAST360 Security BOX

Un livre blanc réalisé par Speedfire mediArchitects
www.speedfire.com / 08 70 27 64 00